IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
BEAUMONT DIVISION

KEITH MILLER, *Plaintiff*, VS. JOANNA SOPHIA, NASDAQGL, and JOHN DOES 1 – 20, *Defendants*.	§ § § § § § § § § §	CIVIL ACTION NO. 1:25-CV-00035 JUDGE MICHAEL J. TRUNCALE

ORDER GRANTING PLAINTIFF'S EMERGENCY MOTION FOR *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER AUTHORIZING EXPEDITED DISCOVERY

Plaintiff Keith Miller filed an Emergency Motion for *Ex Parte* Temporary Restraining Order and Order Authorizing Expedited Discovery (the "Motion") [Dkt. 2], in which he seeks an order requiring the freezing of the accounts associated with five deposit addresses at several cryptocurrency exchanges and authorization to issue subpoenas to various third parties likely to be in possession of information about the Defendants. The Court has reviewed Plaintiff's Motion and finds that, for the reasons set out therein, he faces a risk of irreparable harm if the requested relief does not issue and notice to the Defendants should not be required. Accordingly, Plaintiff's Motion is hereby **GRANTED**.

I. BACKGROUND

Plaintiff's relevant allegations are as follows. In June 2024, Joanna Sophia contacted Mr. Miller via Facebook. [Dkt. 1 at ¶ 13]. The two struck up a connection and began messaging regularly. *Id.* Sophia eventually told Mr. Miller about her success investing and trading cryptocurrencies and introduced him to a platform called NASDAQgl. *Id.* at ¶ 14. Sophia told Mr. Miller that she knew how to make profits using NASDAQgl and offered to teach him how to do the same. *Id.* Sophia encouraged Mr. Miller to make a NASDAQgl account, which he soon did. *Id.*

Over the next several months, Sophia "trained" Mr. Miller in cryptocurrency trading using the NASDAQgl platform. *Id.* at ¶ 15. When Mr. Miller was ready to make a deposit on NASDAQgl, the platform provided him asset-transfer instructions via the platform's customer-service chat or on its "deposit" page. *Id.* Mr. Miller completed the transactions as instructed. *Id.* Each time, the amount of the funds he "deposited" would then be reflected in his transaction history and account balance on the NASDAQgl platform. *Id.* Over time, he sent assets to NASDAQgl with a dollar-denomiated value of $635,000.00. *Id.* Mr. Miller's balance on the NASDAQgl platform appeared to grow rapidly—eventually showing that he had crypto assets worth more than $128,000,000.00 in his account. *Id.* at ¶ 16. But when he attempted to withdraw his funds, NASDAQgl informed him that him that he could not do so. Mr. Miller soon realized that he had been scammed. *Id.*

Mr. Miller alleges that the NASDAQgl platform was never a "trading platform" of any sort. *Id.* at ¶ 17. It was a simulacrum of a trading platform where no actual trading or investment ever occurred. *Id.* The account balances, the purported profits, and the transaction history displayed were real only in the sense that they reflected the monies Mr. Miller sent to the Defendants. *Id.* And this was simply to ensure that the platform appeared to be functioning. *Id.* The assets Mr. Miller transferred to the Defendants were never "deposited" on NASDAQgl. *Id.* They were never used for cryptocurrency trading—they were simply stolen. *Id.*

Evidentiary materials submitted by Mr. Miller suggest that these kinds of investment scams are now amongst the most prevalent forms of cybercrime worldwide. [Dkt. 2-1 (Declaration of Evan Cole providing excerpts from FBI Internet Crime Report)]. These materials also show that Mr. Miller's experience is very similar to the experiences of other pig-butchering victims described in journalistic outlets and law-enforcement reports. *Id.* at Exs. A (article describing typical pig-butchering scam), B (Secret Service Bulletin describing pig-butchering scams), C (excerpts from FBI Internet Crime Report).

After retaining counsel, Mr. Miller's blockchain investigator performed a "blockchain tracing" report. This "tracing" refers to the process of following digital assets from location to location on the blockchain via publicly available data. [Dkt. 2-1 at ¶ 9]. Mr. Miller's investigator was able to trace his allegedly stolen assets to addresses associated with four distinct cryptocurrency exchanges: (1) Bitkub, (2) Bybit, (3) B2C2, and (4) Coinbase. *Id.*; *see also id.* at Ex. F (tracing report). In the instant Motion, Mr. Miller asks the Court to order that these exchanges temporarily freeze the accounts associated with the blockchain addresses he has identified as receiving the assets stolen from him, so that he might preserve some assets for recovery. [Dkt. 2].

In addition, by investigating NASDAQgl's website, Mr. Miller has identified several additional third parties he claims are likely to be in possession of information about the Defendants. [Dkt. 2 at 25–26; Dkt. 2-1 at ¶ 11]. These third parties include, for example, the companies this website used for web hosting. His Motion seeks to issue subpoenas to these third parties, in addition to the four cryptocurrency exchanges mentioned above, with the aim of revealing the Defendants' true identities and unearthing contact information that he might subsequently use to serve or otherwise communicate with them. [Dkt. 2].

II. ANALYSIS

Mr. Miller has met the requirements for issuance of a temporary restraining order and expedited discovery for the following reasons.

A. Temporary Restraining Order

The standard for issuance of an *ex parte* temporary restraining order has both procedural and substantive elements. Procedurally, the Court has the authority to issue an *ex parte* restraining order where (i) "specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and (ii) "the movant's attorney certifies in writing any efforts made to give notice and why it should not be required." Fed. R. Civ. P. 65(b)(1)(A)–(B).

Both requirements are met here. Mr. Miller's Verified Complaint, the Cole Affidavit, and the blockchain-tracing report show the likelihood of immediate and irreparable injury or loss. These materials suggest that Mr. Miller was in fact the victim of a prevalent form of cybercrime—the "pig-butchering scam"—which features well-established and recognizable patterns of deception. *See* [Dkt. 1 at ¶¶ 13–17; Dkt. 2-1 at ¶¶ 3–6 (concluding that Mr. Miller was the victim of a pig-butchering scam and providing news reports and law-enforcement bulletins for comparison)]. The Cole Declaration further details how the assets allegedly stolen from Mr. Miller could be further transferred to unretrievable locations at any time, with the click of a button. [Dkt. 2-1 at ¶¶ 6–7 (explaining that crypto assets can be "dissipated at any moment, with a few mouse clicks and keyboard strokes," and that Mr. Miller will be unlikely to recover his assets if they are further dissipated)]. Several federal courts, including this Court, have found that this exigency justified issuance of *ex parte* restraining orders in similar crypto-fraud cases, and this Court finds their reasoning persuasive here.[1]

In addition, Mr. Miller's attorney has certified why notice should not be required. *See* [Dkt. 2 at 16–17; Dkt. 2-2 (Declaration by Attorney Marshal Hoda)]. As Mr. Miller points out in his Motion, the Court has the authority to enter an *ex parte* order not only where notice to the adverse party is impracticable, but where "notice to the defendant would render fruitless [the] prosecution of the action." *In re Vuitton et Fils S.A.*, 606 F.2d 1, 5 (2d Cir. 1979); *see also, e.g.*, *First Tech. Safety Sys., Inc. v. Depinet*, 11 F.3d 641, 650 (6th Cir. 1993) (noting that *ex parte* order is justified where "the adverse party has a history of disposing of evidence or violating court orders or [] persons similar to

[1] *See, e.g.*, *Harris v. Upwintrade.com*, 1:24-cv-00313-MJT, Dkt. 7 (E.D. Tex. Aug. 8, 2024) (Truncale, J.) (granting TRO in functionally identical pig-butchering case); *Cohn v. Popescu*, No. 1:24-cv-00337, 2024 WL 4525511 (E.D. Tex. Aug. 16, 2024) (Truncale J.) (same); *Ohlin v. Defendant 1*, No. 3:23cv8856-TKW-HTC, 2023 WL 3676797, at *3 (N.D. Fla. May 26, 2023) ("Considering the speed with which cryptocurrency transactions are made as well as the anonymous nature of those transactions, it is imperative to freeze the Destination Addresses to maintain the status quo to avoid dissipation of the money illegally taken from Plaintiffs."); *Jacobo v. Doe*, No. 1:22-CV-00672DAD-BAK (BAM), 2022 WL 2052637, at *3 (E.D. Cal. June 7, 2022) ("Because it would be a simple matter for [defendant] to transfer [the] cryptocurrency to unidentified recipients outside the traditional banking system and effectively place the assets at issue in this matter beyond the reach of the court, the court finds that plaintiff is likely to suffer immediate and irreparable harm in the absence of injunctive relief.") (cleaned up); *Astrove v. Doe*, No. 22-CV-80614-RAR, 2022 WL 2805315, at *3 (S.D. Fla. Apr. 22, 2022) (same).

the adverse party have such a history"). Under this logic, courts have found that notice of an asset-freeze motion is not required if the parties to be enjoined "are likely to dissipate assets and destroy business documents," such that the very act of providing notice would "cause immediate and irreparable injury, loss, or damage to [the] Court's ability to award effective final relief." *Fed. Trade Comm'n v. Dluca*, No. 18-60379-CIV, 2018 WL 1830800, at *2 (S.D. Fla. Feb. 28, 2018), *report and recommendation adopted*, 2018 WL 1811904 (S.D. Fla. Mar. 12, 2018). Several courts have found that this same reasoning justified issuance of *ex parte* freezing orders in crypto-fraud cases analogous to this one.[2]

Here, the thrust of Mr. Miller's allegations is that the Defendants are professional cybercriminals who have every motivation to place their ill-gotten gains beyond the reach of this Court or any other authority. *See generally* [Dkts. 1, 2]. While at this stage these are simply allegations, Mr. Miller has provided sufficient evidence to suggest that the Defendants will in fact further dissipate assets if they were given notice of his Motion. This is sufficient to justify issuance of an *ex parte* order under these unique circumstances.

Having found that the procedural requirements for issuance of an *ex parte* restraining order are met, the Court now turns to the substantive standard. To obtain a temporary restraining order, a movant must show (1) a substantial likelihood of success on the merits, (2) a substantial threat of irreparable harm if the injunction does not issue, (3) that the threatened injury outweighs any harm that will result if the injunction is granted, and (4) that the grant of an injunction is in the public

[2] *See, e.g.*, *Gaponyuk v. Alferov*, No. 2:23:CV-01317-KJM-JDP, 2023 WL 4670043, at *2 (E.D. Cal. July 20, 2023) (issuing *ex parte* asset-freeze TRO in similar crypto-fraud case, and writing that "federal district courts have granted *ex parte* relief in situations like this one, noting the risks that cryptocurrencies may rapidly become lost and untraceable."); *Ohlin*, 2023 WL 3676797, at *2 (notice not required where plaintiff offered declarations showing that the defendants were crypto-criminals, which gave the court "every reason to believe the Defendants would further hide those [stolen] assets if they were given notice"); *Jacobo*, 2022 WL 2052637, at *3 (notice not required because plaintiff made credible allegations that defendants were crypto-criminals, which "pose[d] a heightened risk of asset dissipation").

interest. *Moore v. Brown*, 868 F.3d 398, 402–03 (5th Cir. 2017) (per curiam) (citing *Byrum v. Landreth*, 566 F.3d 442, 445 (5th Cir. 2009)).

Mr. Miller has met each of these requirements. On the merits, Mr. Miller makes claims against the Defendants for violation of the Racketeering Influenced and Corrupt Organizations Act ("RICO"), fraud, and conversion. [Dkt. 1 at ¶¶ 20–31]. He has alleged and provided evidence that the Defendants deceived him and misappropriated his assets in what appears to have been an intentional scam. *Id.* at ¶¶ 1–4, 13 – 17; [Dkt. 2-1 at ¶¶ 3–5]. The Court finds, at this stage, that the similarities between Plaintiff's allegations and the widely known characteristics of this distinctive kind of scam suggest that he will indeed be able to prevail on these claims once a full evidentiary record is developed. In addition, the Court notes that the asset freeze Mr. Miller seeks in this instance is permissible in light of his request for a constructive trust over specific, traceable stolen assets, as several courts have held in analogous cryptocurrency-fraud cases. *See, e.g.*, *Yogaratnam v. Dubois*, No. CV 24-393, 2024 WL 758387, at *3 (E.D. La. Feb. 23, 2024) (issuing asset-freeze TRO in crypto-fraud case, noting that "numerous district courts . . . have issued a TRO in this exact circumstance to freeze a cryptocurrency asset," and collecting cases); *Jacobo*, 2022 WL 2052637, at *3 (issuing asset-freezing TRO where plaintiff sought constructive trust over allegedly stolen assets); *Gaponyuk*, 2023 WL 4670043, at *2 (same).

Mr. Miller has also shown that irreparable harm will ensue absent the restraining order he seeks, for the same reasons explained above. In light of the speed with which cryptocurrency transactions are made, as well as the potential that the Defendants may further move the assets they are alleged to have stolen, the Court finds that Mr. Miller's request to freeze the exchange accounts to which those assets were transferred is justified, as have other courts in similar cases. *See Jacobo*, 2022 WL 2052637, at *3, 5.

Next, the Court finds that the threatened injury to Mr. Miller outweighs any harm the Defendants may suffer by virtue of a freeze of their accounts. Maintaining the assets at the destination

accounts is perhaps Mr. Miller's only realistic chance at a future recovery in this case. In contrast, the Defendants will suffer at worst a temporary inability to move assets if the injunction is later dissolved. *See id.* at *6 ("A delay in defendant's ability to transfer the [allegedly stolen] assets only minimally prejudices defendant, whereas withholding injunctive relief would severely prejudice plaintiff by providing defendant time to transfer the allegedly purloined assets into other accounts beyond the reach of this court.").

Finally, the Court finds that issuing the injunction is in the public interest. Mr. Miller has adduced evidence showing that he is but one of many victims of what appears to be a wave of similar scams. [Dkt. 2-1 at ¶¶ 3–5 (Cole Declaration describing pig-butchering scams as "epidemic" and providing law-enforcement and academic materials suggesting that Americans have lost billions to such scams)]. A freezing order will serve the public interest here both by dissuading would-be fraudsters from preying on American citizens, and "providing assurance to the public that courts will take action to promote . . . recovery of stolen assets when they can be readily located and traced to specific locations." *Jacobo*, 2022 WL 2052637, at *6 (cleaned up) (citation omitted); *see also, e.g.*, *Gaponyuk*, 2023 WL 4670043, at *3 (finding that asset freeze would "serve the public's interest in stopping, investigating, and remedying frauds").

B. Expedited Discovery

Typically, parties may not seek "discovery from any source before the parties have conferred as required by Rule 26(f)." Fed R. Civ. P. 26(d)(1). But expedited discovery before a Rule 26(f) conference is permitted where "authorized … by court order." *Id*. Courts in this circuit apply a "good cause" standard to determine whether such an order should issue. *St. Louis Grp., Inc. v. Metals & Additives Corp*., 275 F.R.D. 236, 239 (S.D. Tex. 2011) (applying good cause standard). Good cause may be found where "the need for expedited discovery in consideration of the administration of justice, outweighs the prejudice to the responding party." *Id*. (citation omitted).

Many courts, including this Court, have authorized expedited discovery from cryptocurrency exchanges in cryptocurrency-related fraud cases like this one. *See, e.g.*, *Harris*, No. 1:24-cv-00313-MJT, at p. 14 (authorizing expedited discovery); *Cohn*, 2024 WL 4525511, at *5 (same); *Strivelli v. Doe*, No. 22-cv-22060, 2022 WL 1082638, at *2 (D.N.J. Apr. 11, 2022) (authorizing expedited discovery from cryptocurrency exchanges in crypto case and noting "the Court's review of cryptocurrency theft cases reveals that courts often grant motions for expedited discovery to ascertain the identity of John Doe defendants."); *Licht v. Ling*, No. 3:23-CV-1018-X, 2023 WL 4504585, at *4 (N.D. Tex. June 20, 2023) (issuing broad authorization for expedited discovery in functionally identical crypto-fraud case and requiring that "any party served with a request for production shall produce all requested items within 72 hours of the request").

Here, Mr. Miller's proposed discovery arises from his pre-suit blockchain tracing and investigation of the Defendants' web property. *See* [Dkt. 2 at 26–27]. These investigations revealed a series of third parties likely to be in possession of information about the Defendants. Each of those third parties and their connections to this case are set out below.

Subpoena Target	***Connection to Case***
Bitkub	Plaintiff alleges that this exchange is associated with one or more of the Target Addresses in this matter.
Coinbase	Plaintiff alleges that this exchange is associated with one or more of the Target Addresses in this matter.
B2C2	Plaintiff alleges that this exchange is associated with one or more of the Target Addresses in this matter.
Bybit	Plaintiff alleges that this exchange is associated with one or more of the Target Addresses in this matter.
NameSRS	Plaintiff has identified several additional websites that are associated with NASDAQgl. Name SRS is the domain-name registrar for several of these sites.
Gname	Gname is alleged to be the domain-name registrar for NASDAQgl.com.

Google	NASDAQgl is alleged to have communicated with Keith Miller via the email address nasdaq.otc.dep@gmail.com.
Meta	The alleged scam began with a message to Keith Miller from Joanna Sophia via Facebook. Keith then communicated with Joanna on WhatsApp. Both Facebook and WhatsApp are owned by Meta Platforms, Inc.
JivoChat	NASDAQgl used JivoChat's LiveChat for the customer-service chat on its website.
Cloudflare	NASDAQgl.com is alleged to have used Cloudflare's content delivery network.

Mr. Miller requests the Court's authorization to issue subpoenas to each of the above-listed entities seeking the following information. For all targets, Mr. Miller seeks to discover all biographical and contact information associated with the Defendants' accounts. He also seeks to discover IP-address and location logs showing the devices and locations from which the Defendants accessed these accounts.

Mr. Miller also seeks to discover any payments information in the subpoena targets' possession, including the Defendants' transaction histories and information about the credit or debit cards the Defendants used to pay for the subpoena targets' services. As to the Defendants' payment methods, Mr. Miller seeks only information sufficient to identify the Defendants' payments provider and the Defendants' account with that provider.

Finally, as to the firms to which the Mr. Miller's assets are alleged to have been transferred—*i.e.*, Bitkub, Coinbase, B2C2, and Bybit—Mr. Miller seeks to discover the current account balances associated with the Defendants' accounts, their transaction histories, and identification of any other accounts on the respective platforms associated with the accountholders by re-use of biographical or contact information.

Courts have authorized similar discovery where the plaintiff adduced evidence that the persons about whom the information was sought were cybercriminals and the plaintiff also sought a temporary restraining order freezing the assets held in those accounts. *Strivelli*, 2022 WL 1082638,

at *2 (granting broad expedited discovery in functionally identical crypto-fraud case); *see also Licht*, 2023 WL 4504585, at *3–4 (same). The Court finds these courts' reasoning persuasive and therefore authorizes the scope of discovery requested by Mr. Miller here.

III. RELIEF REQUESTED

A. Restraining Order

Plaintiff has submitted evidence tracing the assets he alleges were stolen from him to five deposit addresses at the cryptocurrency exchanges Bitkub, Bybit, B2C2, and Coinbase (the "Receiving Addresses"). The Receiving Addresses are:

Exchange	**Address**
Bitkub	0x3d1d8a1d418220fd53c18744d44c182c46f47468
Bitkub	0x80260a115ca1b7ab7a7a8e8e747bc14f78170720
Bybit	0xf614c8da40d87b16a04150ec36fbc23e8f303aaf
B2C2	0xa29e963992597b21bcdcaa969d571984869c4ff5
Coinbase	0x51ae6ded70713e72925fb2b819d0916ab75ff364

For the reasons set out in the Motion, the Court finds that the accounts associated with these deposit addresses should be frozen. Accordingly, the Court hereby **ORDERS** that Defendants and their agents, servants, employees, attorneys, partners, successors, assigns, and all other persons or entities through which they act or who act in active concert or participation with any of them, who receive actual notice of this Order by personal service or otherwise, whether acting directly or through any trust, corporation, subsidiary, division or other device, or any of them, are hereby restrained from withdrawing, transferring, or encumbering any assets currently held by, for, or on behalf of the persons

controlling the accounts associated with the above-listed Receiving Addresses, or any business entity through which they act or which acts in active concert or participation with them; including but not limited to those assets currently held at or for the Receiving Addresses.

In accordance with Fed. R. Civ. P. 65(b)(2), this Order will expire fourteen (14) days from its entry unless it is extended for good cause shown. No bond shall be required to be posted by Plaintiff.

B. Expedited Discovery

The Court finds that Plaintiff's request to issue expedited discovery should be granted for the reasons set out in the Motion. Plaintiff is authorized to serve subpoenas on the following third parties (1) Bitkub Online Co., Ltd; (2) Coinbase Global, Inc.; (3) B2C2, Ltd.; (4) Bybit Fintech Ltd.; (5) Name SRS AB; (6) GNAME.com PTE. Ltd.; (7) Alphabet, Inc.; (8) Meta Platforms, Inc.; (9) Jivosite, Inc.; and (10) Cloudflare, Inc.

In light of the time-sensitivity of Plaintiff's subpoenas to the cryptocurrency exchanges to which his assets were ultimately transferred, Plaintiff is further authorized to serve this Order and his subpoenas on these exchanges via email directed to the following addresses.

Recipient	**Service Address**
Bitkub Online Co., Ltd.	support@bitkub.com bitkubchain@bitkub.com
B2C2, Ltd.	regulatory@b2c2.net london@b2c2.net
Bybit Fintech, Ltd.	compliance@bybit.com legal@bybit.com

All subpoenaed parties shall produce the materials sought in the subpoena to Plaintiff's counsel within seven (7) days of their receipt of Plaintiff's subpoena and this Order.

The Court finds that any privacy interest the Defendants have in the documents requested by Plaintiff is outweighed by the need to investigate and prosecute the theft and conversion alleged in the complaint. Such privacy concerns shall not be good cause for the subpoenaed party to withhold the requested material.

SIGNED this 25th day of February, 2025.

Michael J. Truncale
United States District Judge